Nonorthogonal decoy-state Quantum Key Distribution

Jing-Bo Li, and Xi-Ming Fang*

Department of Physics, Hunan Normal University,
Changsha 410081, People's Republic of China

(Dated: February 1, 2008)

In practical quantum key distribution (QKD), weak coherent states as the photon source have a limit in secure key rate and transmission distance because of the existence of multiphoton pulses and heavy loss in transmission line. The decoy-state method and the nonorthogonal encoding protocol are two important weapons to combat these effects. Here, we combine these two methods and propose an efficient method that can substantially improve the performance of QKD. We find a 78 km increase over the prior record using the decoy-state method and a 123 km increase over the result of the SARG04 protocol in transmission distance.

PACS numbers: 03.67.Dd

Quantum key distribution (QKD)[1, 2] allows two users, Alice and Bob, to communicate in absolute security in the presence of an eavesdropper, Eve. Unlike conventional cryptography, the security of QKD is based on the uncertainty principle and the noncloning theorem [3]. In other words, the measurement of an unknown quantum state modifies the state itself. Thus, Eve cannot gain any information on the key without introducing any error in the correlations between Alice and Bob. However, in practical implementations, an attenuated laser pulse (a weak coherent state)is often used as the source. The existence of multiple photon pulses, even though very rare, poses a serious problem for the security of the protocol, especially in high lossy channel. An eavesdropper (Eve) can in principle have the full information of Bob's sifted key by using the photon-number-splitting (PNS)attack [4, 5, 6]: Eve blocks all single-photon pulses and part of multi-photon pulses and separates each of the remained multi-photon pulses into two parts therefore each part contains at least one photon. She keeps one part and sends the other part to Bob, through a lossless channel.

Recently, two important methods have been proposed to overcome PNS attacks. One is the decoy-state method firstly proposed by Hwang [7], and further studied by Wang [8], and also Lo and co-workers [9, 10]. Particularly, by combining the idea of the entanglement distillation approach by Gottesman, Lo, Lutkenhaus, and Preskill (GLLP) [11] with the decoy state method, they achieved a formula for secure key generation rate [9]:

$$S \geq q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}, \qquad (1)$$

where q is the sifting efficiency depending on the implementation (1/2 for the BB84 protocol, because half the time Alice and Bob bases are not compatible), Q_μ and E_μ are the gain (i.e., counting rate [8]) and quantum bit error rate (QBER) of the signal state respectively, and can be measured directly, Q_1 and e_1 are the gain and QBER of single-photon states respectively, and can be estimated by using decoy state method, $f(E_\mu)$ is the error correction efficiency [12], and H_2 is the binary Shannon entropy, given by:

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x). \qquad (2)$$

The other is the nonorthogonal states encoding protocol proposed by Scarani, Acin, Ribordy and Gisin (SARG04) [13], which uses exactly the same four states as in BB84 [2], and only the classical sifting procedure is different from BB84: instead of revealing the basis, Alice announces publicly a pair of nonorthogonal states. Thus, Eve needs at least three photons to obtain full information. This means one can utilize the two-photon part to generate a secure key. However, either the decoy state method or the nonorthogonal states encode protocol has no further security analysis on it.

In this paper, we first present a simple method that can study the secure key generation rate when single-photon and two-photon pulses are employed to generate secure key. The structure of the paper is as follows. First, we derive a formula for secure key generation rate, where two-photon part is included. Next we present a simple method that will give a tight bound to Q_0, Q_1, e_1, Q_2 (the gain of two-photon states)and e_2 (the error rate of two-photon states) respectively. Then we present the advantage of this new protocol at secure key generation rate and transmission distance by comparing with the results in [9]. Finally, we discuss and conclude.

Our new GLLP formula. The secure generation rate must include the two-photon part when we use SARG04 protocol. So we need to modify Eq. (1) to satisfy our purpose.

Theorem The key generation of an nonorthogonal encoding scheme is given by:

$$S \geq q\{-Q_\mu H_2(E_\mu)+Q_0+Q_1[1-H_2(e_1)]+Q_2[1-H_2(e_2)]\}, \qquad (3)$$

where q is 1/4 for SARG04, and Q_0 is the gain of the vacuum signals.

Now, let us prove it. According to the Csiszár-Körner theorem [14]: if the mutual information Alice-Bob is

*corresponding author: Email: fxm601@yahoo.com.cn larger than either the mutual information Alice-Eve or Bob-Eve, then Alice and Bob can distil a secret key. The secure key generation in QKD satisfies

$$S \geq I(A:B) - I(B:E), \tag{4}$$

where $I(A:B)$ and $I(B:E)$ are mutual information of Alice-Bob and Bob-Eve respectively, and are given by:

$$\begin{aligned} I(A:B) &= qQ_\mu(1 - H_2(E_\mu)) & (5) \\ I(B:E) &= q\{Q_1H_2(e_1) + Q_2H_2(e_2) + \sum_{n\geq 3} Q_n\}, & (6) \end{aligned}$$

where Q_n is the gain of n-photon states, and q is 1/4 for SARG04. The vacuum signals do not contribute to it at all because of the mutual information of vacuum being zero. Here, we take the most conservative assumption that Eve has all the information on all tagged pulses (the parts for photon number $n \geq 3$) and obtains full information stemming from the QBERs e_1 and e_2. Combining Eq. (4) and $Q_\mu = \sum_{n\geq 0} Q_n$, we get the result of our theorem. In fact Eq. (3) can be generalized from Lo's theorem [15] directly if only adding the secure generation rate of the two-photon part. As discussed in [9], practical error correction protocols are generally inefficient. Thus, the secure key generation rate for practical protocols is given by:

$$\begin{aligned} S \geq q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_0 + Q_1[1 - H_2(e_1)] \\ +Q_2[1 - H_2(e_2)]\}. \quad (7) \end{aligned}$$

The optimal secure key generation rate without decoy states. Although we have obtained the Eq. (7) that can calculate the secure key generation rate for the SARG04 protocol, we have to discard the it due to the presence of Eve. In this case, Eve can block all single-photon pulses or all two-photon pulses, she can get more information, so the worst secure key generation rate is given by

$$S_{worst} = \frac{1}{4}(-Q_\mu f(E_\mu)H_2(E_\mu) + Q_0 + \Omega Q_\mu[1 - H_2(\frac{e}{\Omega})]), \tag{8}$$

where $f(E_\mu) = 1$ for convenience, and Ω, the fraction of untagged photons, satisfies

$$\Omega = 1 - \frac{(1 + \mu + \mu^2/2)e^{-\mu}}{Q_\mu}. \tag{9}$$

S_{worst} is optimised if we choose $\mu = \mu_{optimal}$, which fulfills

$$\eta e^{-\eta\mu_{optimal}} = \frac{1}{2}\mu^2_{optimal}e^{-\mu_{optimal}}. \tag{10}$$

Since for realistic setup we expect that $\eta \ll 1$, we find $\mu_{optimal} \approx \sqrt{2\eta}$.

The lower bound of the secure key generation rate with decoy states. A verified lower bound of secure key generation rate can be obtained by using decoy-state method. This method is dependent on the real-world QKD protocols deeply. In practical implementations, a weak coherent state (i.e., a dephased coherent state) is a mixed state of

$$\rho = \int \frac{d\theta}{2\pi}|\sqrt{\mu}e^{i\theta}\rangle\langle\sqrt{\mu}e^{i\theta}| = \sum_n P_n(\mu)|\mu\rangle\langle\mu|, \tag{11}$$

where $P_n(\mu) = \frac{\mu^n e^{-\mu}}{n!}$ and μ is the mean photon number. The gain, Q_μ, and QBER, E_μ, are given by

$$\begin{aligned} Q_\mu &= \sum_{n\geq 0} Q_n & (12) \\ Q_\mu E_\mu &= \sum_{n\geq 0} Q_n e_n & (13) \end{aligned}$$

and $Q_n = Y_nP_n(\mu)$, where e_n and Y_n are respectively the error rate and yield of the n-photon state. In the normal case that there is no eavesdropper, Q_μ and E_μ are given by [10]:

$$\begin{aligned} Q_\mu &= Y_0 + 1 - e^{-\eta\mu}, & (14) \\ Q_\mu E_\mu &= e_0Y_0 + e_{det}(1 - e^{-\eta\mu}), & (15) \end{aligned}$$

where e_{det} is the probability that a photon hit the erroneous detector, η is the overall transmission probability of a photon.

In the presence of an eavesdropper, Eve, we can use the decoy-state method to detect Eve's attacks. The essence of decoy state idea is that Eve cannot distinguish the decoy state from the signal state. So the signal state and the decoy state have the same values for the yield, Y_n, and QBER, e_n. In order to achieve the unconditional security of QKD with the key generation rate given by Eq. (7), we must consider now how to use the decoy state idea to estimate Q_0, Q_1, e_1, Q_2 and e_2. A similar problem for orthogonal encoding protocols has been analyzed explicitly by Lo and his co-workers in [10]. Here we exploit their method to solve the question in nonorthogonal protocols.

For simplicity, we propose a specific protocol that uses only four decoy states: vacuum and three weak decoy states. The vacuum can be used to estimate the background rate,

$$\begin{gathered} Y_0 = Q_{vacuum}, \\ e_0 = E_{vacuum} = \frac{1}{2}. \end{gathered} \tag{16}$$

The dark counts occur randomly; thus the error rate of the the dark count is 1/2. The signal and three decoy states with expected numbers μ, ν_1, ν_2 and ν_3 satisfy

$$\begin{gathered} 0 < \nu_3 < \nu_2 \leq \frac{2}{3}\mu < \nu_1 \leq \frac{3}{4}\mu, \\ \nu_1 + \nu_2 > \mu, \\ \nu_2 + \nu_3 < \mu. \end{gathered} \tag{17}$$

Alice and Bob will get the following gains and QBERs for signal state and these three decoy states:

$$
\begin{aligned}
Q_\mu e^\mu &= Y_0 + Y_1\mu + \frac{Y_2\mu^2}{2} + \sum_{i=3}^{\infty} Y_i \frac{\mu^i}{i!},\\
E_\mu Q_\mu e^\mu &= e_0Y_0 + e_1Y_1\mu + \frac{e_2Y_2\mu^2}{2} + \sum_{i=3}^{\infty} e_iY_i \frac{\mu^i}{i!},\\
Q_{\nu_1} e^{\nu_1} &= Y_0 + Y_1\nu_1 + \frac{Y_2\nu_1^2}{2} + \sum_{i=3}^{\infty} Y_i \frac{\nu_1^i}{i!},\\
E_{\nu_1} Q_{\nu_1} e^{\nu_1} &= e_0Y_0 + e_1Y_1\nu_1 + \frac{e_2Y_2\nu_1^2}{2} + \sum_{i=3}^{\infty} e_iY_i \frac{\nu_1^i}{i!},\\
Q_{\nu_2} e^{\nu_2} &= Y_0 + Y_1\nu_2 + \frac{Y_2\nu_2^2}{2} + \sum_{i=3}^{\infty} Y_i \frac{\nu_2^i}{i!},\\
E_{\nu_2} Q_{\nu_2} e^{\nu_2} &= e_0Y_0 + e_1Y_1\nu_2 + \frac{e_2Y_2\nu_2^2}{2} + \sum_{i=3}^{\infty} e_iY_i \frac{\nu_2^i}{i!},\\
Q_{\nu_3} e^{\nu_3} &= Y_0 + Y_1\nu_3 + \frac{Y_2\nu_3^2}{2} + \sum_{i=3}^{\infty} Y_i \frac{\nu_3^i}{i!},\\
E_{\nu_3} Q_{\nu_3} e^{\nu_3} &= e_0Y_0 + e_1Y_1\nu_3 + \frac{e_2Y_2\nu_3^2}{2} + \sum_{i=3}^{\infty} e_iY_i \frac{\nu_3^i}{i!}.
\end{aligned}
\tag{18}
$$

Alice and Bob can estimate the lower bound of Y_1 and the upper bound of e_1 from Eq. (18) by using decoy states ν_2 and ν_3 . The lower bound of Y_1 is given by

$$
\begin{aligned}
Q_{\nu_2}e^{\nu_2} - Q_{\nu_3}e^{\nu_3} &= Y_1(\nu_2-\nu_3) + \textstyle\sum_{i\geq 2}\frac{Y_i}{i!}(\nu_2^i-\nu_3^i)\\
&\leq Y_1(\nu_2-\nu_3) + \textstyle\frac{\nu_2^2-\nu_3^2}{\mu^2}\sum_{i\geq 2}\frac{Y_i\mu^i}{i!}\\
&= Y_1(\nu_2-\nu_3) + \textstyle\frac{\nu_2^2-\nu_3^2}{\mu^2}(Q_\mu e^\mu - Y_0 - Y_1\mu).
\end{aligned}
\tag{19}
$$

Here,in order to prove the inequality in Eq. (19), we have made use of the inequality that $a^i - b^i \leq a^2 - b^2$ whenever $0 < b < a \leq \frac{2}{3}$, and $i \geq 2$. The last equality sign holds in the in Eq. (19) if and only if Eve raises the yield of two-photon states and blocks all the states with photon number greater than 2. In fact Eve will not take this tactics because she cannot achieve full information on two-photon state. The upper bound of e_1 is given by

$$
\begin{aligned}
E_{\nu_3}Q_{\nu_3}e^{\nu_3} &= e_0Y_0 + e_1Y_1\nu_3 + \textstyle\sum_{i=2}^{\infty} e_iY_i\frac{\nu_3^i}{i!}\\
&\geq e_0Y_0 + e_1Y_1\nu_3.
\end{aligned}
\tag{20}
$$

By solving Eq. (19) and Eq. (20), the lower bound of Y_1 and upper bound of e_1 are given by

$$
\begin{aligned}
Y_1 &\geq Y_1^L\\
&= \frac{\mu^2(Q_{\nu_2}e^{\nu_2} - Q_{\nu_3}e^{\nu_3}) - (\nu_2^2-\nu_3^2)(Q_\mu e^\mu - Y_0)}{\mu^2(\nu_2-\nu_3)(\mu-\nu_2-\nu_3)},\\
e_1 &\leq e_1^U = \frac{E_{\nu_3}Q_{\nu_3}e^{\nu_3} - e_0Y_0}{Y_1^L\nu_3}.
\end{aligned}
\tag{21}
$$

Then, according $Q_1 = Y_1P_1(\mu)$, the gain of single-photon states is given by

$$
Q_1 \;\geq\; Q_1^L = Y_1^L\mu e^{-\mu}. \tag{22}
$$

Next, Alice and Bob can estimate the lower bounds of Y_2 and the upper bound of e_2 respectively by using decoy states ν_1, ν_2 and ν_3 from Eq. (18) under conditions Eq. (17). The lower bound of Y_2 is given by

$$
\begin{aligned}
&Q_{\nu_1}e^{\nu_1} - Q_{\nu_2}e^{\nu_2}\\
&= Y_1(\nu_1-\nu_2) + \textstyle\frac{Y_2}{2}(\nu_1^2-\nu_2^2) + \sum_{i\geq 3}\frac{Y_i}{i!}(\nu_1^i-\nu_2^i)\\
&\leq Y_1(\nu_1-\nu_2) + \textstyle\frac{Y_2}{2}(\nu_1^2-\nu_2^2) + \frac{\nu_1^3-\nu_2^3}{\mu^3}\sum_{i\geq 3}\frac{Y_i\mu^i}{i!}\\
&= Y_1(\nu_1-\nu_2) + \textstyle\frac{Y_2}{2}(\nu_1^2-\nu_2^2)\\
&\quad + \textstyle\frac{\nu_1^3-\nu_2^3}{\mu^3}\sum_{i\geq 3}(Q_\mu e^\mu - Y_0 - Y_1\mu - \frac{Y_2\mu^2}{2})\\
&= \textstyle\frac{Y_2}{2}(\nu_1^2-\nu_2^2) + \frac{\nu_1^3-\nu_2^3}{\mu^3}\sum_{i\geq 3}(Q_\mu e^\mu - Y_0 - \frac{Y_2\mu^2}{2}).
\end{aligned}
\tag{23}
$$

In order to prove the inequality in Eq. (23), we have made use of the inequality that $a^i - b^i \leq a^2 - b^2$ whenever $0 < b < a \leq \frac{3}{4}$, and $i \geq 3$. The last equality sign holds in Eq. (23) if and only if Eve raises the yield of three-photon states and blocks all the states with photon number greater than 3. In addition, to obtain the last sign equality in Eq. (23), we have let ν_1 and ν_2 satisfying

$$
\nu_1 - \nu_2 - \frac{\nu_1^3 - \nu_1^3}{\mu^2} = 0. \tag{24}
$$

The upper bound of e_2 is given by

$$
\begin{aligned}
E_{\nu_3}Q_{\nu_3}e^{\nu_3} &= e_0Y_0 + e_1Y_1\nu_3 + \textstyle\frac{e_2Y_2\nu_3^2}{2} + \sum_{i=3}^{\infty} e_iY_i\frac{\nu_3^i}{i!}\\
&\geq e_0Y_0 + \textstyle\frac{e_2Y_2\nu_3^2}{2}.
\end{aligned}
\tag{25}
$$

By solving Eq. (23) and Eq. (25), the lower bound of Y_2 and Q_2 and upper bound of e_2 are given by

$$
\begin{aligned}
Y_2 &\geq Y_2^L\\
&= \frac{2\mu(Q_{\nu_1}e^{\nu_1} - Q_{\nu_2}e^{\nu_2}) - 2(\nu_1-\nu_2)(Q_\mu e^\mu - Y_0)}{\mu(\nu_1-\nu_2)(\nu_1+\nu_2-\mu)},\\
Q_2 &\geq Q_2^L = \frac{Y_2^L\mu^2e^{-\mu}}{2},\\
e_2 &\leq e_2^U = \frac{2E_{\nu_3}Q_{\nu_3}e^{\nu_3} - 2e_0Y_0}{Y_2^L\nu_3^2}.
\end{aligned}
\tag{26}
$$

Now, the lower bound of the secure key generation rate, according to Eq. (7), is given by:

$$
\begin{aligned}
S^L = q\{&-Q_\mu f(E_\mu)H_2(E_\mu) + Q_0 + Q_1^L[1-H_2(e_1^U)]\\
&+Q_2^L[1-H_2(e_2^U)]\},
\end{aligned}
\tag{27}
$$

where $Q_0 = Y_0e^{-\mu} = Q_{vacuum}e^{-\mu}$. Comparing our result (given in Eq. (7)) with the prior result in [10](given in Eq. (1)), we see that the main difference is that in our result, two additional terms, Q_0 and $Q_2^L[1-H_2(e_2^U)]$, can also generate secure keys. To fix the ideas, we will compare our protocol with the SARG04 protocol and BB84 protocol according Eqs. (7) (8) and (1) respectively in the following paragraph.

For simplicity, We only consider the asymptotic case (i.e. omit statical fluctuations of Q_n and e_n). By using

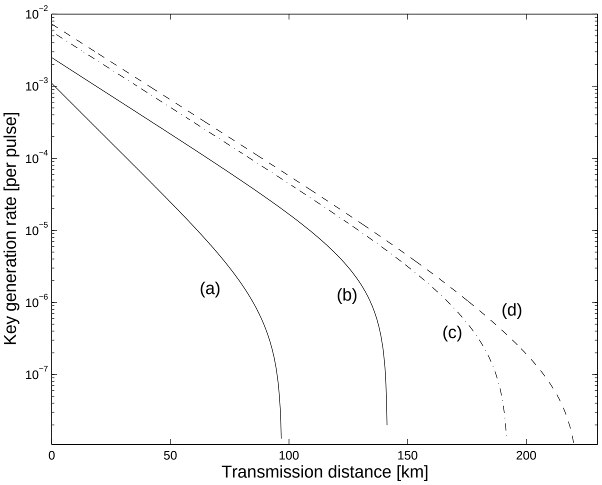

FIG. 1: (a)The optimal secure generation rate for SARG04 protocol without decoy states, (b)The optimal secure generation rate for BB84 protocol with decoy states ($\mu = 0.48$), (c) The secure generation rate for our protocol by using the formula (27)($\mu = 0.48$), (d) The secure generation rate for our protocol by using the formula (27) ($\mu = 0.30$). The parameters is given according to experiment GYS [16]: $\alpha = 0.21dB/km$, $e_{det} = 3.3\%$, $Y_0 = 1.7 \times 10^{-6}$, and the detection efficiency of Bob's setup $\eta_Bob = 0.045$. $f(E_\mu) = 1.22$.

the GYS [16] experiment as an example, the result shows in Fig. 1. The curve (a) is the optimal secure generation rate for SARG04 protocol without decoy states achieved by using Eq. (8). The curve (b) is a simple repeat of Ref. [9] for BB84 protocol with decoy states. We note that our protocol is better than both SARG04 protocol without decoy states and Lo's protocol at any distance. The maximal distances of the three protocols are 220, 142, and 97 km respectively. Theoretically, we can achieve a longer transmission distance with our method when we decrease the value of μ. In these cases, however, the weak decoy state method cannot work efficiently due to the statical fluctuations.

In summary, we have proposed an efficient and feasible nonorthogonal decoy-state protocol to do QKD over very lossy channel. we have clearly demonstrated how to estimate the lower bound of the secure key generation rate in this new protocol. Our result shows that, the combination of decoy state method and nonorthogonal states encoding protocol can make great progress at the secure key generation rate. Our protocol can be realized easily because it is the same as Lo's protocol in operation.

J.-B.Li thanks Xiongfeng Ma for his kind help with numerical calculations. This work is supported by Scientific Research Fund of Hunan Provincial Education Department No. 03c213.

[1] N. Gisin, G. Ribordy, W. Tittel, & H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[2] C. H. Bennett, & G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, IEEE, 1984, pp. 175-179.

[3] W. K. Wootters and W. Zurek, Nature (London) **299**, 802 (1982).

[4] B. Huttner, N. Imoto, N. Gisin, and T.Mor, Phys. Rev. A **51**, 1863 (1995).

[5] N. Lütkenhaus, Phys. Rev. A **61**, 052304, (2000).

[6] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus, and M. Jahma, New. J. Phys. **4**, 44 (2002).

[7] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[8] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005); X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).

[9] H.-K. Lo, X.-F. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[10] X.-F. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[11] D. Gottesman, H.-K. Lo, N. Lütkenhaus, & J. Preskill, Quantum Info. and Comp. **4**, No.5 (2004) 325-360.

[12] G. Brassard, & L. Salvail, *Advances in Cryptology, Eurocrypt' 93 Proceedings* (1993), pp. 410-423.

[13] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[14] I. Csiszár and J. Körner, IEEE Trans.Inf. Theory **IT-24**, 339 (1978).

[15] H.-K. Lo, quant-ph/0503004.

[16] C. Gobby, Z. L. Yuan, & A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).